Risks by Using COTS Products and Commercial ICT Services

(March 2000)

Susanne Jantsch
IABG mbH
Einsteinstrasse 20
D - 85521 Ottobrunn, Germany

Introduction

Among the requirements influencing today's procurement of new information and communications systems, the most prominent are

- cost effectiveness
- use of the latest developments in information and communications technology (ICT)

through the whole lifetime of a system. This can no longer be achieved in procurement procedures as they used to be, with long planning and development phases, resulting in proprietary products based more and more often on out-dated technology at the time they go operational. Also, storage or provision of spare parts for and maintenance of such fully or mainly proprietary systems, as well as the education and training of personnel for their operation and maintenance, are increasingly cost intensive.

The alternative and inevitable approach is the consequent use of COTS products, allowing for easy and timely release changes and introduction of new hard and software versions when they come to market, paired with the consequent outsourcing of all those services which are available with comparable or higher quality by non-military providers, allowing usually to choose among competitive offers.

However, though on first view this new way of procurement seems to perfectly meet the above mentioned requirements for cost effectiveness and application of the latest ICT developments, there is also a new class of risks to be identified and dealt with.

After summarizing the eminent advantages of the consequent use of COTS products and outsourcing, this paper will address the risks that have to be considered and finally point out methods to improve confidence in how to use "unsecure" products and services.

Benefits of COTS Products and Outsourcing

Innovation rates in modern ICT keep decreasing at a breathtaking pace, while at the same time new developments continuously broaden the spectrum of service details and technical features waiting to be introduced into new or refined products. Integration and diversification occur in parallel, allowing to design and produce in large numbers products adapted or adaptable to very specific customer requirements.

As an example, we see today mobile phones more and more equipped with services / interfaces for services like WAP and SMS, allowing to use a piece of hardware originally designed to communicate via speech to send and receive written messages and to retrieve information from the internet. On the other hand, the spectrum of available mobile handsets and contracts differing in service details leads to such a fast change of products (as a combination of hardware, software, and service) offered by service providers to the enormously increasing number of mobile phone users all over the world that a market analysis may easily be outdated within three months.

This example illustrates the ever changing variety of often highly competitive products openly available on the ICT market.

Competition helps in both keeping the prices low or bringing them down and in the products constantly being made more attractive by add-ons, by featuring the latest technological developments, and in the case of complex systems by add-ons like customisable services for configuration, maintenance, update integration, migration from or to other products / product versions.

Thus, the definition of requirements for ICT components and even for complex ICT systems need no longer result in lengthy design and development phases, but can be accompanied by quick though intensive market reviews and tests, which may be followed by quick procurement decisions based fully or largely on commercial products with or without lifetime maintenance.

The advantages both for end users as for system administrators are plentiful. From the user perspective, for example, common place graphical user interfaces facilitate getting used to a new system or to new applications in an existing system, since features present in many applications are accessed more and more often in the same form, so that the user can easily identify and concentrate on new and unknown features to be used.

Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.

For the administrators, the advantages range from having access to "frequently asked questions" and provider hotlines and thus often well tested solutions helping with day to day problems typical for the product over the better availability of bug fixes for widely spread products as compared to having little or no support for a system that was only devised in one or very few pieces, to the possibility of fully concentrating on user oriented administrative tasks by outsourcing tasks like maintenance, release changes or similar tasks so that they no longer intermingle with the daily routines.

The benefits of outsourcing tasks and services formerly performed within an organisation become obvious when such tasks are only needed from time to time, when equipment needed for these tasks is costly but only infrequently used, when the people responsible for these tasks need special, cost and time intensive training but have little opportunity to use their skills etc. If these tasks and services can be done by outside providers without the need of being familiar with the daily routines of the system or organisation, outsourcing may lead to a less costly and more professional performance of systems.

But even ICT services needed constantly are more and more often subject to outsourcing, as e.g. wide area communications services, customer support (hotline), system administration.

Another example for outsourcing is the operation of systems where, especially in a military environment, high rates for personnel changes are opposed to a long and extensive training required. In such a case, the continuity of systems operation can be better achieved by constant assignment of external specialists.

Other candidates for outsourcing are power supply, water supply, where the label "commercial service" comes into play with the increasing privatisation of these sectors, or services like facility management which may include the employment of private security services.

Paradigm shift in procurement

To profit from the described benefits of using COTS products and commercial services, in many countries the military has already adopted a strategy to use COTS products wherever possible. However, the subsequent changes needed in the procurement processes for new systems as well as for replacing or enhancing existing proprietary systems, sometimes even systems not yet fully operational (and with designed lifetimes of another five or ten years), with COTS products have not yet in all of these countries been fully accomplished.

Another development is that military systems can no longer be easily separated in ICT and non-ICT systems. Electronically interconnecting systems that used to be isolated and only dependent on people to transfer information from one to the other, or introducing and continuously improving "intelligence" in weapon systems via embedded systems, electronic sensors etc., automating logistics, setting up automated chains of interdependent information processes with growing complexity as part of decision support processes allowing, e.g., increasingly real-time situational awareness, are just a few examples showing that information and communications technology has become almost omnipresent in all military systems.

And there is yet another aspect to interconnection and interdependence: the number of systems to which commercial services as e.g. energy supply or wide area communications are indispensable continuously increases, leading to inevitable dependencies of military systems from and interconnection of military systems with systems and services from the civil sector.

Risks by use of COTS products and commercial services

Both the adoption of the maxim of consequent use of COTS products where adequate products are available, and the fact of increased interconnectivity and interdependency within the military and between the military and the non-military sectors lead to new classes of risks.

These classes of risks comprise technical risks as well as risks from organisational, procedural, even political origins, which may, for example, originate from

- System inherent risks due to complexity and heterogeneity of system components, including bugs, backdoors, manipulated chips etc.
- Increasing vulnerability and attack options by interconnecting systems with one another and with commercial open networks (Information Warfare),
- Dependence on products not implemented under military control, which thus have to be operated as "black boxes"
- Dependence on suppliers of equipment and services that operate world wide and whose performance may be unpredictable.
- Political risks when a product is completely or partly produced in a country that is not a friend or partner or changed from friend to adversary
- Risks by using products or integrating products into existing systems that do not meet all the requirements originally formulated for a certain task
- Loss of support and continuity when the manufacturer or a product line with "guaranteed" availability cease to exist

The same range of problems have to be considered when commercial services are used, be it just sporadically or as an essential component of a military system of service. Here, it is also crucial to recognise and take apply appropriate measures against problems that may arise from:

- External personnel having direct or indirect access to military systems, e.g. via direct or remote maintenance,
- external personnel having access to people via social engineering techniques,
- risks introduced by sporadic unavailability of services supposed to "always" available, and
- risks caused by attacks on normally highly reliable services indirectly affecting systems or services depending thereon.

Risk assessment and risk management

In dealing with these problems, the solution cannot be to simply avoid the origins of these risks, e.g. by avoiding the use of COTS products. They have to be accepted as an inevitable side-effects of the need to use COTS products and commercial services, and it has to be acknowledged that these side-effects have to be dealt with. We have to learn to assess and manage these risks as a part of daily life.

To be able to deal with these risks, however, we have to understand that *all* of these risks really have to be recognised and consciously acknowledged as *risks* at all organisational levels.

It is not enough to have IT security experts deal with typical IT security risks, although achieving a high standard of IT security by implementing and managing well tuned and harmonised IT security measures is a fundamental part of successful risk management.

In the October 1999 symposium, I described a threat model and suggested possible procedures (see [1]) for a holistic security management. In the conclusion, I said: " Security management should be designed to effectively assure and support operation of a system (of systems), including all the processes it is designed for. It should be based on a „holistic" view of all security aspects to enhance abilities to detect and correctly assess irregularities and to invoke adequate countermeasures."

Managing security (i.e. managing the measures to achieve the goal) is in this context equivalent to managing risks (i.e. dealing with the problems and keeping them low), where the word "management" indicates not one time actions and static solutions, but continuous analysis of protocols, reviewing the efficiency of technical and organisational measures and procedures, acceptance by the users and so on.

Managing security within an organisation also should be equivalent to enabling secure use of systems and services made available within the organisation

For dealing with risks in connection with the use of COTS products and commercial services, this means that the grade of security (from unsecure to secure) of every specific system or service – as a whole or as a component – has to be assessed and taken into account during the installation or integration by adequate technical and / organisational and /or procedural measures.

Technical aspects

The use of "secure" products, e.g. evaluated along the Common Criteria, is only sometimes a solution, as new releases would have to be re-evaluated and the evaluation process is time and resource consuming, preventing that the latest technology can be made available in a "secure" product at (almost) the same time as the equivalent "normal" product. Also, "secure" products are much more expensive than their "normal" counterparts, which may have a considerable impact on the cost effectiveness and thus means that every day "normal" products have no real alternative.

Technical measures to reduce risks are more and more often based themselves on COTS products and services, e.g. by use of firewalls, anti-virus software, intrusion detection systems, commercial computer emergency response services and so on, where the quality and reliability of these products is very often mainly based on shared positive experience with the product and, for reasons of rapid changes to continuously adapt to new threats, only rarely on evaluation.

However, technical measures may be weakened, if not useless if negligence and carelessness of both users and administrators cannot be considerably reduced. To achieve this, a considerable rise in awareness of the existing risks is required.

Awareness

An overarching risk assessment and subsequent risk management can only be successfully achieved when all parties involved in all stages of the life cycle of ICT systems, i.e. in requiring, designing, deploying, and finally using these systems or the information provided by them, which means more or less everybody, are aware of the imminent problems and willing to take responsibility in the risk management process.

Awareness in this context means

- recognising and acknowledging the existence of a new quality of risks created by the consequent use of COTS products and commercial services

- recognising and acknowledging that these risks have to be dealt with in a co-operative way,
- willingness to contribute to risk reduction according to one's position and tasking
- consequent use of existing security measures
- encouragement of everybody else to do so as well,
- attention to unusual events or obvious security breaches,
- ...

Although these characteristics are independent of whether the systems are pure COTS or using many or few or no COTS components, or of whether they are connected to other systems or to commercial networks, it has to be understood that to cope with the risks induced by increasingly interconnected and interdependent COTS-based ICT systems and direct or indirect use of commercial services, a high level of awareness not just with the security people is a precondition for a successful risk management that enables secure use of these inherently "unsecure" products and services.

This high level of awareness from the simple user through to the highest management level has to be reached step by step, including the broader coverage of security issues in education and training as an integral part of learning how to use and operate a system, supported by a variety of exercises both for crisis management training and for evaluating whether present technical and organisational measures are appropriate to deal with critical events.

A prerequisite for adequate awareness is the availability of comprehensive but easily understandable information on risks, on security measures, on how they work, on possible effects of omitting or ignoring security measures and so on.

Conclusion

For successful risk management, an important prerequisite is to achieve interaction and co-operation between people at all levels: Reports should be encouraged

- of obvious incidents as well as of unusual behaviour – no report should be laughed at or carelessly put aside,
- on events someone has caused himself – helping to reduce or solve a problem should be valued much higher than "finding and punishing the culprit"

but also on successful events such as

- successful integration of "unsecure" products – how to configure them, what sort of extra measures are used,
- new measures that improve early detection of events or increase the number of successfully rejected attacks etc.

Accepting that the use of COTS products and commercial services will continuously increase in the military environment, the obvious benefits have to be levelled with not quite as obvious risks on one hand and, on the other hand, with the possibilities available and duties unavoidable to actively manage these risks.

References

[1] S. Jantsch: "Assessing threats and vulnerabilities", presented at the NATO RTA/IST Symposium "Protecting NATO Information Systems in the 21st Century", Washington D.C., 25.-27.10.1999